hierarchy can include: consuming application, point of claim, followed by authentication credential strength. In such examples, session-related context parameters provide a mechanism to apply overrides, which can occur after the application of role-related context parameters. Session-related context parameters can operate as a set of rules that are applied after the role-related context parameters are considered. In some examples, session-related context parameters will not vary, as they can be common to all consumer applications. Role-related context parameters can vary by role.

[0029] Points of claim include, for example, customer use through the Internet, customer use through a corporate LAN, third party access, and/or any combination thereof. Authentication credential strength can vary among users. For example, customers accessing applications through a typical PIN login mechanism can be authorized to access a greater number of resources than, for example, customers accessing applications through a single sign-on protocol from a corporate LAN.

[0030] The "resolve role" process **304** of FIG. **3** includes determining (**304**) a role associated with an actor and resolving (**304**) the scope of authorized action for the actor. An actor's role is determined (**304**) based, for example, on the identity of the actor **202***a* and the one or more pre-defined context parameters that have been obtained (**303**). For example, the actor can have a pre-defined context parameter of "ABC Client Corporation." Based on the actorID **202***a* and the "ABC Client Corporation" pre-defined context parameter, the actor is assigned a role of "manager" within the "ABC Client Corporation."

[0031] A policy type is associated (**305**) with the role of an actor. A policy type can represent a cohesive collection of one or more policy elements. Policy types are associated with roles, which can be, for example, stored in a policy type-role table **164***c*. A policy type can be associated with many roles, and a role can be associated with many policy types. A policy type can contain the policy elements that relate to a specific authorization area, such as "compensation," "time management," and/or "defined contribution exchange transactions." A policy element can include a single name/value pair that specifies a single authorization setting or decision. Policy elements can specify specific authorization elements, such as whether an actor is allowed to access (access control policy element), view (data view/presentation policy element), and/or act upon (function performance/update operation policy element) an entity, system component, and/or any combination thereof. For example, a policy type named "performance management" might include policy elements such as "access performance management application," "view compensation data," "can increase salary," "maximum salary increase percentage," and/or any combination thereof. The policy type does not have to define the policy element values. In some examples, the policy type named "performance management" would not include values, such as "yes" or "no" for policy elements such as "access performance management application," and/or "view compensation data." In such examples, defining the policy element values is the function of one or more policy instances.

[0032] Existing pre-defined context parameters are read (**306**) and/or one or more other pre-defined context parameters are obtained (**306**) to provide input into the determination (**307**) of one or more policy instances for each policy type associated with a role. An instance of a policy type is mapped (**307**) to a role based on the one or more pre-defined context parameters. A policy instance can be a specific collection of one or more policy elements with values provided for each policy element derived from the policy type and associated with the one or more pre-defined context parameters for a given role. The role, policy instance, one or more pre-defined context parameters, and the resolved scope can, for example, determine (**308**) the one or more resources that are accessible to the user **110**. Determining user access to resources is part of the role-based authorization process.

[0033] FIG. **4** illustrates exemplary details of the process element **304** for role resolution. An actor is mapped (**304***a*) to a role based on one or more pre-defined context parameters. A role scope is associated (**304***b*) with a role. Such associations can be stored, for example, in the role scope-role table **164***b*. For a given role there can be one or more role scopes. A role scope can be associated with a role and used as the basis for defining the actor-role scope for a role assignment. The role scope can define the format of the actor-role scope (the actor-role scope elements) required when a user **110** is assigned to a role. The role scope includes, but is not limited to, the actor-role scope format, required actor-role scope values, optional actor-role scope values, default actor-role scope values, and/or mandatory actor-role scope values.

[0034] The actor-role scope format can describe what the actor-role scope entities are and the data types for these entities. In some examples, the role scope can flag values as "required" during role assignment. In such examples, the system **100** will not save the role assignment record **200** without these required values being populated. The role scope can define optional or wildcard values. These actor-role scope values can be optionally specified at the time of role assignment. If these values are not specified, then any value could apply for the given actor-role scope element. The role scope can define default values. These values apply if the role assignment process does not provide explicit values. The role scope can include mandatory actor-role scope values which include values that apply to every role assignment and cannot be changed. For example, the role of "employee" can have a mandatory role scope value of "self." The role assignment process may not provide a different value for this mandatory role scope value.

[0035] The actor-role scope key can be derived (**304***c*) from the general specification of scope contained within the role scope associated with the role of a user **110**. The actor-role scope key provides a pointer to the scope values maintained by, for example, a customer recordkeeping system. The actor-role scope key includes one or more pointers to the populations and/or entities that an actor is authorized to act upon. The scope includes the populations and/or entities themselves, which can be comprised of one or more sets of values. The actor-role scope key describes how to obtain the scope from the role-based authorization system. For example, a actor-role scope key may describe a specific location within an organization, e.g., cost center **84325**, the relationship to the actor, e.g., people who report to the actor, and/or the depth of the relationship, e.g., all organizational levels down. For example, the scope associated with cost center **84325** resolves to a list of subordinate employees within the cost center that include employee numbers 003-03-0003, 002-02-0002, and 001-01-0006.